Office of the Army Chief Information Officer/G-6

ARMY NETWORK CAMPAIGN PLAN

2020 & BEYOND

February 2015

Version 1.2

CIO/G-6

ENABLING SUCCESS FOR TODAY & TOMORROW

U.S.ARMY

CIOG6.ARMY.MIL

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

CHANGES

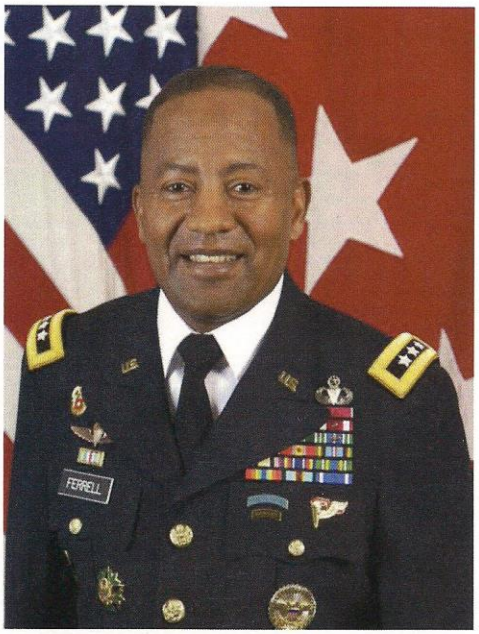
Refer requests for all changes that affect this document to: Architecture, Operations, Networks and Space (SAIS-AON), CIO/G-6, ATTN: Mr. Edwin Payne, 107 Army Pentagon, Washington, DC 20310-0107.

Table of Contents

This page intentionally left blank.

Intent

To enable a globally responsive and regionally aligned Army, the network and the Signal force must adapt to meet the business and expeditionary mission command needs of joint force commanders across the full range of military operations in a joint, inter-organizational, multinational partner environment. The Army will deploy lighter, more mobile command posts to austere environments that will securely connect to the network and access information – whether at home station, en route, upon early entry or in a mature theater of operations.



LTG Robert S. Ferrell
Chief Information Officer/G-6

The Army is already well on the way to achieving the vision of a secure, integrated, standards-based information environment. LandWarNet is evolving to eliminate redundancy and close security gaps by becoming inherently joint. We are leading the transition away from Service-centric approaches toward joint information technology acquisition, ownership and administration, and the delivery of end-to-end enterprise capabilities as described by the Joint Information Environment (JIE) construct. The Army will continue to leverage industry advances in cloud and mobile technologies to create a global network that is a platform for cyberspace operations. To ensure that we enable success, my top priorities for network modernization are:

- Optimize Signal force capabilities by properly structuring, training, equipping and integrating the Signal Regiment and cybersecurity workforce.
- Enhance cybersecurity strategy, architecture, policy, resourcing, doctrine and capabilities as we transition to a joint regional security architecture and align with the JIE construct to exponentially improve network security against external and insider threats.
- Increase network throughput and ensure sufficient computing infrastructure to effectively support operating and generating force information needs.
- Develop strategy, policy and resources to deliver information technology services to the tactical edge.
- Strengthen network operations through comprehensive situational awareness of network performance and security at all echelons as we transition to the Joint Management System (JMS).

The Army, along with mission partners and stakeholders are working to provide the robust network necessary for commanders to apply strategic land power and achieve security and force protection in all mission settings. Everything we do enables success, today and tomorrow, for our warfighters to fight and deploy anytime, anywhere – making us Army Strong!

Robert S. Ferrell
Lieutenant General
Chief Information Officer/G-6

Overview

The network is one of the key technological focus areas described in the Army Operating Concept (October 2014). As an enabler of situational understanding across the joint force, the network must "empower leaders at the lowest levels with relevant combat information, situational understanding, and access to joint and Army capabilities." The Army Operating Concept calls for developing and modernizing "capabilities, such as cloud-enabled networks for mobile operations in austere environments and across wide areas," that are "simple and resilient, anticipating enemy efforts to disrupt communications."

The world is evolving into an increasingly interconnected environment. The Army of 2020 will operate in a complex world where cloud-based computers receive data from tens of billions of devices. These computers will have the capacity to digest, correlate, contextualize, process and then present data back to humans in a way that assists our decision-making process. The Army is modernizing its network to prepare for the impending data-driven, cloud-based world, as depicted in Figure 1. While legacy networking architectures stored and protected data locally, cloud-based architectures will store and protect data in a centralized yet distributed repository that enables global access. The Army Network Campaign Plan outlines current efforts that posture the Army for success in a cloud-based world.

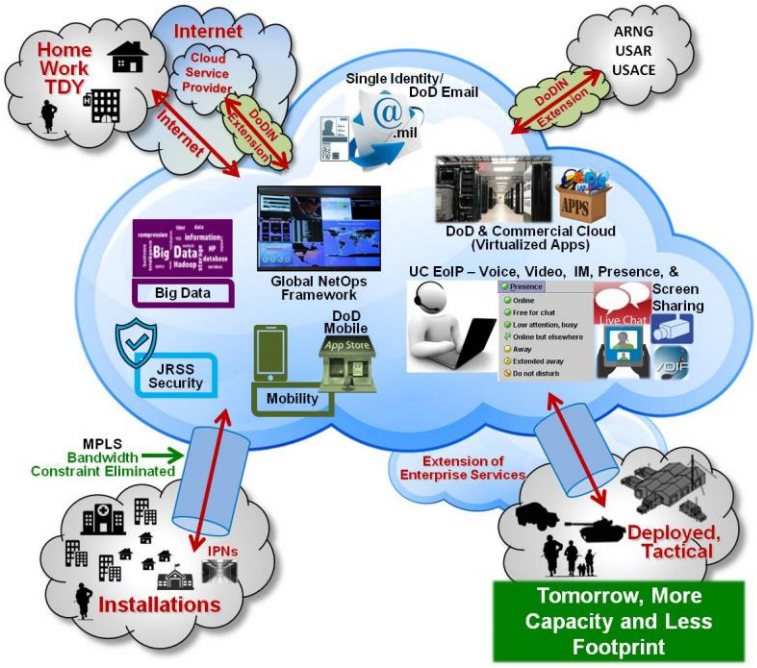


Figure 1: The Army Network of Tomorrow

The Army is following Industry best practices to transition to the cloud. Cloud-based networking requires assured and sufficient bandwidth. The Army is employing Multi-Protocol Label Switching (MPLS) and other transport upgrades designed and to increase exponentially increase the throughput of our global 'backbone' and the connectivity to posts, camps and stations. With Joint Regional Security Stacks (JRSS), the Army is transitioning from legacy security that protected data locally and required hundreds of security stacks to regionalized security that protects data in the cloud. The Army's application rationalization project will help reduce the number of applications the Army maintains (currently more than 25,000), and it will modernize and move the remaining applications to the cloud. Once bandwidth is sufficient, security is applied and data/applications reside in the cloud, the Army will then provide secure access to data from mobile devices. The end state is a global cloud-based network designed to provide Soldiers access to tailored and timely information at the point of need. As the network aggregates, processes, secures and presents data in a way that is easily understood, Soldiers will be able to make informed, more effective decisions as they perform the missions of the future.

Purpose

The Army Network Campaign Plan (ANCP) supports The Army Plan and the Army's Operating Concept. The ANCP:

- Defines the CIO/G-6's vision, mission and roles for the Army's network.
- Clarifies the strategic environment facing the Army.
- Introduces the Chief Information Officer/G-6 Lines of Effort (LOEs), desired end states and supporting objectives.
- Provides an Army Network Initiatives Roadmap.

"The Army Operating Concept calls for regionally engaged Army forces to establish a global landpower network, shape security environments, and prevent conflict. Army operations are inherently cross-domain operations. Army forces contribute to the joint force mission accomplishment by providing foundational capabilities that permit effective integration of military, intergovernmental, and multinational efforts."

This campaign plan supports mission readiness by providing the vision and direction that set conditions for and lay a path to Network 2020 and Beyond, thereby unifying efforts to provide a modern network that meets the Army's warfighting and business needs, today and tomorrow. The ANCP is comprised of this and two additional documents, which are intended to be used together to achieve the overall vision. The *ANCP Implementation Guidance, Near-Term* (revised annually) describes execution activities and is updated to reflect the changing realities of Army budget, acquisition, resources and mission. The *ANCP Implementation Guidance, Mid-Term* (updated annually) charts network modernization from a capabilities perspective in order to guide resource planning and shape the Program Objective Memorandum.

Delivering network capabilities to the Army is a team effort. Segments of LandWarNet have traditionally been modernized independently to support operating and generating forces. Achieving the vision of a secure, integrated, standards-based and globally accessible network that enables Army success in the joint fight today and tomorrow demands a fully coordinated and synchronized approach across the community. The Army will align with the Joint Information Environment to bring even greater network capability and interoperability that would not have been possible for an individual service. The ANCP is the overarching "game plan" that drives our focus and unifies our team effort to ***optimize operational effectiveness, increase network*** and ***information security*** while ***achieving increased efficiencies***.

Vision

The network of 2020 and Beyond must enable the Army to train as it fights and deploy on little to no notice anytime, anywhere, in austere environments. As such, it is core to a smaller, more capable, better-trained expeditionary Army. The network of the future is:

> A secure, integrated, standards-based environment that ensures uninterrupted global access and enables collaboration and decisive action throughout all operational phases across all environments.

The network envisioned spans all Army operations, from administrative operations in garrison to the most forward-deployed Soldier at the tactical edge. Army users expect to securely access the network at the point of need — and that the network will deliver. For this reason, the network must be highly responsive, providing the information necessary to execute decisive actions anytime, anywhere and on any device. It also must enable command posts to be mobile, agile, modular, scalable and survivable in support of continuous mission command to win in the complex world in which the Army operates.

Mission Statement

> The CIO/G-6 leads Army network modernization to deliver timely, trusted and shared information for the Army and its mission partners.

The Army CIO/G-6 sets the strategic direction and provides oversight of information resource management, IT policy, integrated IT architecture, Army Enterprise Network (AEN) governance, information protection and cybersecurity, and network and Signal operations.

CIO/G-6 Roles

> The CIO/G-6 defines overall Army network modernization plans and recommends priorities for the resourcing of network modernization activities.

The CIO/G-6 is organized around three directorates: Architecture, Operations, Networks and Space (AONS), which develops Army IT strategy and IT integrated architecture, and manages IT infrastructure; Policy and Resources (P&R), which oversees IT policy and governance, capital planning, investment management and enterprise service management; and Cybersecurity, which develops and manages cybersecurity strategy, identifies potential network risks and associated impacts and mitigation based on Army objectives, and oversees policies and processes to ensure adherence to security standards. Second Army is a direct reporting unit (DRU) that operates, maintains and defends the Army network.

Operating Environment

In the complex world described in the Army Operating Concept, the network operating environment presents ever-evolving threats and opportunities. Even as network capabilities enable the Army to conduct successfully business and warfighting functions, our adversaries have access to similar technologies with which to avoid our strengths and exploit our vulnerabilities. This and other challenges to development and defense of an "always on, always available" capability require a robust combination of materiel, personnel, processes and policy solutions. From a network perspective, changes in the Army's operating environment are manifested in several major areas: the strategic conditions, fiscal boundaries and technological evolution, which includes the cyberspace mission.

Strategic

Recent and ongoing conflicts reinforce the need to balance the technological focus of Army modernization with recognition of the limits of technology and an emphasis on the human, cultural and political aspects of armed conflict. The strategic environment is characterized by a constantly shifting geopolitical landscape facilitated by the proliferation of information and communications technologies that increase the momentum of human interaction. The Army cannot predict whom it will fight, where it will fight and with what coalition it will fight, so the network must support a broad range of potential missions with a myriad of possible unified action partners. An Army that is globally engaged and regionally aligned requires access at the point of need, robust network capacity, and capability that is tailorable and scalable to support the full range of business and warfighting processes. Net-centric capabilities are key to providing the joint force multiple options, integrating the efforts of multiple partners, operating across multiple domains and presenting enemies multiple dilemmas.

Fiscal

Long lead times for acquisition, programming and budgeting and lack of budgetary predictability characterize the current fiscal environment. The Army must clearly define LandWarNet requirements and standards, and allow suppliers to compete for procurement of their solutions. The culture of controlling all network resources must give way to effectively leveraging joint networks, with more IT capabilities being provided by the joint enterprise. The Army also must establish and maintain a balance between technological advantage over our adversaries and the aggregate cost of IT. Investments in new capabilities must be measured and then prioritized by their ability to significantly improve upon current capabilities, to fill critical capability gaps and to reduce risks to the mission. Divestiture and sun-setting of legacy systems and circuits are critical to allocating enough scarce resources to network modernization.

Technological

The technological environment is characterized by rapid innovation, widespread access to powerful computer processing capabilities that were once restricted to use by government and academia, and persistent and evolving cybersecurity threats.

Rapid changes in technology shorten the useful life of many of the physical components that make up the network. To compensate, a faster, more flexible approach to both acquisition and training is required in order to maintain capability while mitigating vulnerabilities. Such an approach must include security features that are "baked into" systems from the outset and not "bolted on" as an afterthought.

Growing computer processing power presents multiple threats and opportunities. The ability to store tremendous amounts of data, combined with powerful analytical tools, makes it possible to query large distributed collections of loosely structured information to support faster, more intelligent decision making. So-called big data technology will enable the Army to detect or predict previously undetectable anomalies in the network but it may also arm adversaries with the ability to disrupt U.S. operations. Enemy actions may not be easily distinguishable from legitimate activity, and the lack of full visibility across the network creates vulnerabilities and delays detection and response.

Threats will continue to grow in scale and sophistication as access and computing power grow. They range from state-sponsored offensive military operations and espionage activities, to violent extremist organizations intent on disrupting the American way of life, to criminals and recreational hackers seeking financial gain and notoriety. Additionally, in cyberspace, traditional boundaries do not exist and anonymous attacks can occur at near light speed. Given the progression of these advanced persistent threats, we must continuously develop new approaches to managing and securing information, and ensuring our ability to operate and provide our workforce the right capabilities to defend, monitor, detect, isolate and respond to threats in real time.

Network architecture also presents significant challenges. The Army's current network is comprised of top secret, secret and unclassified enclaves, with more than 1,000 external access points. This makes the network as a whole difficult to secure and to manage. The always present pressure to deploy new technology must be balanced against approved requirements, risks and compatibility with the DoD global architecture. The more complex and opaque the network, the greater are the chances of critical, high-impact vulnerabilities, including insider threats.

The technological environment will shape how the Army fights in the cyberspace domain. The Army retains overmatch through combining technologies and integrating them with organizational, doctrinal, leader development, training and personnel policies. To maintain our advantage in the technological environment, we must develop a right-sized, well trained cadre of Signal, Cyber and Intelligence professionals to conduct, support and enable all three lines of cyberspace operations (CO) depicted in Figure 2: Department of Defense Information Network (DoDIN) Operations, Defensive Cyberspace Operations (DCO) and Offensive Cyberspace Operations (OCO). With the establishment of Army Cyber Command, Second Army, the Cyber Center of Excellence (CCoE) and the new Career Field 17 cyber branch, the Army will be able to address the significant challenges of recruiting, training and retaining the people necessary to generate the human capital required for successful cyberspace operations.

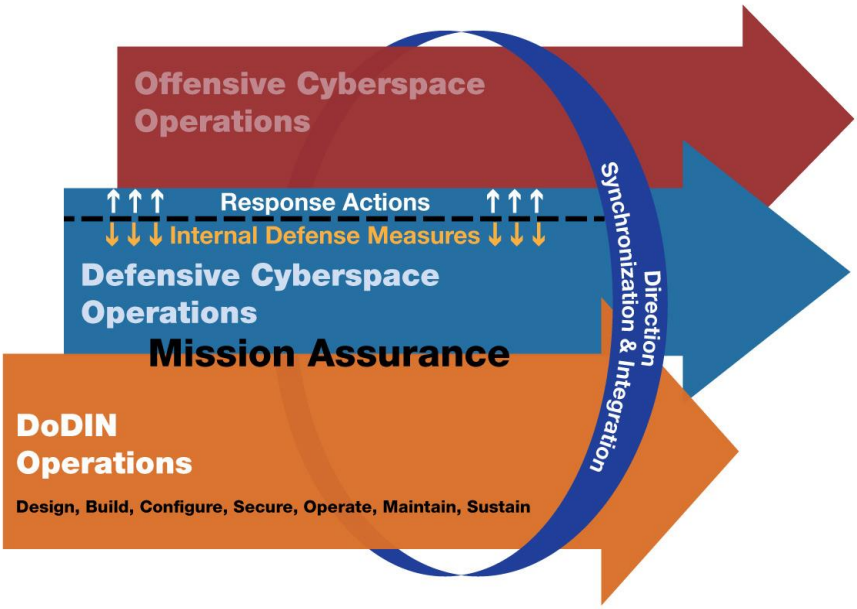


Figure 2: The Three Cyberspace Lines of Operation: DoDIN Operations, DCO and OCO.

The successful execution of cyberspace operations requires the integrated and synchronized employment of offensive, defensive and DoDIN operations, underpinned by effective and timely operational preparation of the environment. Offensive Cyberspace Operations are cyberspace operations intended to project power through the application of force in and via cyberspace. Defensive Cyberspace Operations are cyberspace operations intended to defend DoD or other friendly cyberspace. DoDIN operations are actions taken to design, build, configure, secure, operate, maintain and sustain DoD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, user/entity authentication and non-repudiation.

Strategic Stakeholders

As an organization that focuses on IT strategic planning, architecture development and integration, policy development, investment planning, governance and compliance, the CIO/G-6 works closely with strategic stakeholders to enable the success of the network and achieve common desired end states. Stakeholders represent multiple communities of interest that are involved in modernization of the network. Figure 3 below depicts examples of our stakeholders and mission partners:

Figure 3: Network Stakeholders and Mission Partners

CIO/G-6 Lines of Effort and Desired End States

In the context of this Army Network Campaign Plan, the LOEs serve as the leads for coordinating with community of interest partners to execute network modernization initiatives. The LOEs link tasks, effects and conditions to the network vision and end states. The LOEs and their enabling objectives are aligned to DoD's Joint Capability Areas (JCAs) and complement each other to enable success. Each LOE measures the programs and initiatives it manages for effectiveness, efficiency and attainment of objectives.

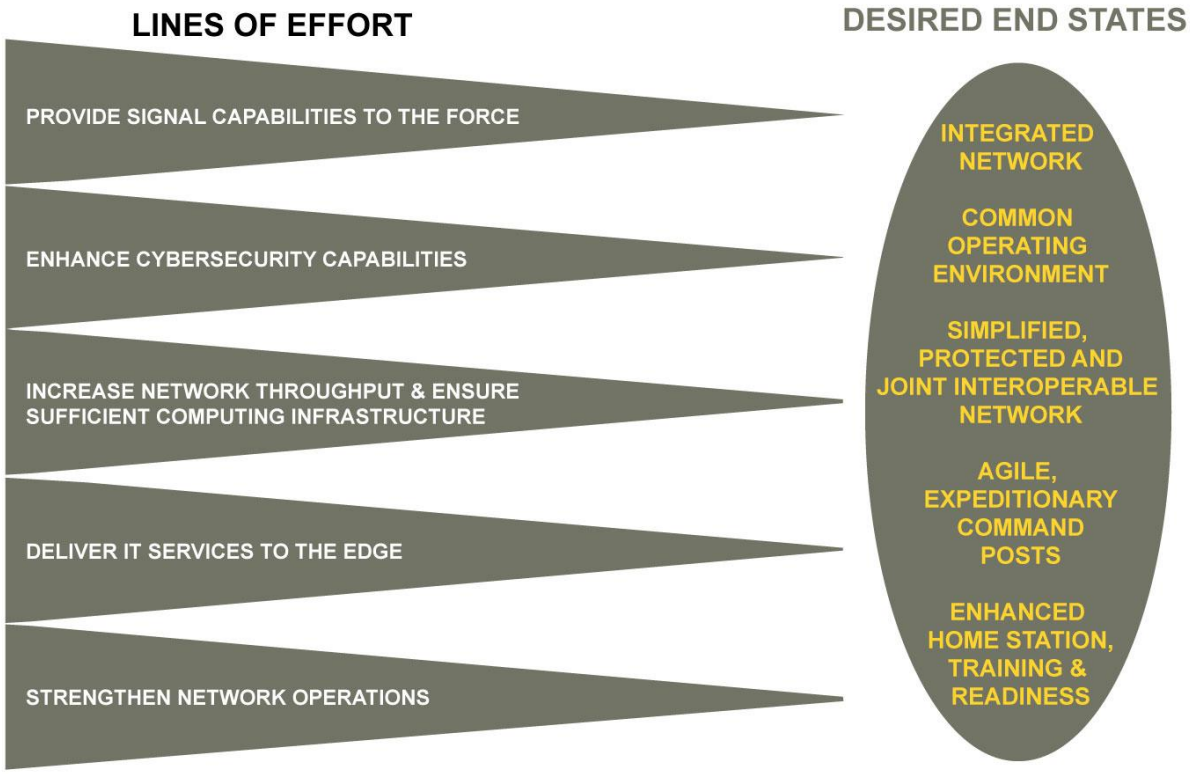


Figure 4: CIO/G-6 Lines of Effort and Desired End States

LOE 1:
PROVIDE SIGNAL CAPABILITIES TO THE FORCE

Goal: Optimize the Signal force to synchronize delivery of future capabilities; and ensure effective operation and defense of a single end-to-end network by continually assessing and shaping doctrine, force structure, and equipping and training concepts across the operating and generating forces.

Desired End State: Signal forces structured, trained and equipped to enable decisive action across the full range of military operations with joint force and unified action partners.

Objective 1.1: Align Signal force structure to ensure support to operational mission priorities.

Objective 1.2: Equip the Signal force to ensure an integrated end-to-end network.

Objective 1.3: Update Signal doctrine to ensure effectiveness, repeatability and relevance.

Objective 1.4: Align training and training support capability to Signal core competencies to ensure maximum effectiveness.

The Signal force encompasses those who influence, manage, operate, maintain and defend the network, including all military, government civilians and contractors. They integrate operating and generating force communications, information processing and management systems into a global information network for the Army and its partners. The Signal force plays an increasingly important role in performing DoDIN Operations and, as part of a combined arms team (Signal, Cyber, Intelligence), defensive cyberspace operations.

LOE 1 will synchronize delivery of network capacity, security, services, training and doctrine to enhance operational capabilities for the Army of 2020. As the Army continues to engage regionally and respond globally, the Signal force must embrace transformational change to support the Army Operating Concept. A holistic examination of Signal formations will be conducted to identify gaps and discover potential mitigating solutions, which, in turn, will influence future force structure. Additionally, a Signal equipping strategy will be developed to deliver intuitive, secured, standards-based capabilities that are adaptive to the commander's requirements and integrated into the common operational environment (COE). The transition to the COE, which is comprised of six computing environments (CE), including Data Center/Cloud and Command Post, will alter Signal operations as we transition from static programs of record to a widget-based applications framework. The Army's functional network owners (Intelligence, Medical, Logistics) must converge networks and leverage common infrastructure, thereby reducing the tactical footprint while gaining efficiencies. The Signal force must be trained and ready, led by innovative, agile, adaptive and professional leaders employing interoperable, reliable technologies that enable distributed, uninterrupted mission command at home station, en route and while deployed. Lastly, doctrinal updates must address technology changes, lessons learned and institutional synergy across the Army network.

Capability-set synchronization and end-to-end modernization activities will leverage institutional enterprise capacity to deliver an interoperable, tailorable, collaborative and accessible network at the point of need. Executing this in a coherent and standardized manner will create opportunities to improve operational effectiveness, enhance security and increase efficiencies, which will enable the shift to a smaller, lighter force that delivers the support necessary to employ Signal capabilities and enable mission command in complex environments.

LOE 2:
ENHANCE CYBERSECURITY CAPABILITIES

Goal: Optimize Defensive Cyberspace Operations and DoD Information Network Operations by continually assessing and shaping cybersecurity strategy, policy, doctrine and resourcing to enhance the security of the network and information environment.

Desired End State: A resilient network and information environment that assure survivability against highly sophisticated cyber adversaries.

Objective 2.1: Increase the resiliency of the network defense posture by minimizing the attack surface, establishing physical path diversity at critical installations, strengthening data defenses and enhancing security through cyber hygiene and best practices.

Objective 2.2: Transform cyberspace defensive operations by deploying capabilities that support passive and active cyberspace defense.

Objective 2.3: Enhance cyberspace situational awareness by improving the cyber-sensing infrastructure, harnessing the power of big data analytics and increasing information sharing.

To meet the challenges of the cyber environment, transformational changes to the Army's cyber culture, workforce, technology, policy and processes are required. The Army must revamp the way it addresses cybersecurity by focusing on mission assurance, rather than solely on compliance. This approach will enable the Army to move beyond bolting on cybersecurity solutions to building resilient, mission-assurance and cybersecurity characteristics into the total information environment. LOE 2 activities will enable the Army to operate effectively in cyberspace while actively defending against adversarial cyber actions. To achieve these objectives, the CIO/G-6 must partner with cyber stakeholders across the Army, DoD, academia and private industry. The CIO/G-6 will leverage the Army Cyber Council to ensure that all mission-critical cyber requirements are validated, prioritized, resourced and rapidly integrated into the Army network.

The Army will establish a regionally aligned Joint Regional Security Stack single security architecture with path diversity to increase mission effectiveness and maintain high levels of operational readiness. We will reduce the network's cyber-attack surface and develop sound architectural principles that include cyber hygiene and best practices to produce a resilient cyber defense posture. Additionally, we will continuously modernize and strengthen our Identity and Access Management and cryptographic capabilities to strengthen data defenses and keep ahead of adversary advances.

It is imperative that we improve our active cyber defense capabilities and situational awareness. Cyber defenders must have capabilities that allow them to discover, detect, analyze and mitigate threats and vulnerabilities in real time as adversarial cyber tactics change. The Army will leverage big data storage and behavioral analytics to uncover previously hidden patterns, correlations and other useful information, enabling us to share and fuse cyber threat indicator data. Additionally, the Army will improve sensors, software and intelligence to detect and stop malicious activity before it can affect the network and systems. We will expand our Information Security Continuous Monitoring (ISCM) capabilities to mitigate and thwart the insider threat.

The CIO/G-6 will continuously collaborate at all levels to share information and enhance cybersecurity awareness, provide ongoing guidance, and shape policy, oversight, and compliance. The CIO/G-6 will also identify opportunities to grow the cybersecurity talent pipeline, promote cybersecurity education and explore professionalization of the cybersecurity career field.

LOE 3:
INCREASE NETWORK THROUGHPUT & ENSURE SUFFICIENT COMPUTING INFRASTRUCTURE

Goal: Lead and integrate Army strategy, policy and resourcing to deliver a robust and secure transport and computing infrastructure that will enable assured warfighting and business operations.

Desired End State: A secure, resilient and versatile global network infrastructure that gives the Army, including regionally aligned forces and unified action partners, the full range of military and business operational advantages across all joint operational phases.

Objective 3.1: Implement the "always on, always available," end-to-end transport infrastructure necessary to meet growing and evolving capacity demands.

Objective 3.2: Transition from disparate data processing and storage solutions to an optimized and responsive global computing and storage infrastructure.

Objective 3.3: Implement a standardized suite of centrally managed end-user devices (EUDs) to improve the user experience and optimize operation and maintenance.

Objective 3.4: Synchronize deployable and fixed network components to provide integrated access to network capabilities.

The global network infrastructure is the physical portion of the network that is responsible for storing, processing and moving information and data. The transport network moves data from the enterprise to the point of need, and includes the terrestrial fiber and wireless infrastructure that extends LandWarNet down to end-user buildings and mobile devices. The computing infrastructure encompasses mobile devices, laptops, desktops and servers that process and store data.

LOE 3 will ensure that the Army is able to meet the ever-increasing information requirements for efficient and effective operations at all echelons. It focuses on providing the conduit for reliable access to mission-critical data when and where needed.

The Army will create a robust and resilient network capable of supporting its information demands through technology that minimizes bandwidth constraints, centralizes computing operations in a common operating environment, and standardizes the provisioning of IT services across the Army. This will reduce the time it takes to deliver information, make available data that were previously inaccessible, standardize delivery of services across the Army, and ensure interoperability with our unified action partners.

This modernized infrastructure will provide the throughput and computing systems required to extend enterprise services and unified capabilities from the institutional network to the tactical edge. The infrastructure will empower garrison-based and distributed mission command, force-generation support activities and distributed live, virtual and constructive training – all of which will enhance the readiness of deployable forces. The infrastructure will also support the rapid evolution and deployment of applications, and provide users connectivity to critical information as they transition between mission environments.

LOE 4:
DELIVER IT SERVICES TO THE EDGE

Goal: Provide a consistent, end-to-end user experience by developing strategy, policy, resources and change management for the transition of IT services from local implementations to enterprise capabilities.

Desired End State: A global environment that offers integrated and timely access to relevant information, services and applications at the point of need.

Objective 4.1: Plan for globally available unified capabilities.

Objective 4.2: Transition to unified capabilities and plan for additional user-facing, globally-available IT services.

Objective 4.3: Integrate enterprise services into the tactical network.

Army core enterprise services are a small set of CIO-mandated services that provide information at the point of need. These services, both user-facing and enabling, give awareness of and access to information. These doctrine, organization, training, materiel, leadership, facilities and policy solutions are provided to the Army enterprise with both institutional and operational components taken into consideration.

Army IT services are not currently provided to users at consistent and acceptable levels of service. LOE 4 will improve the level of service for users while reducing inefficiencies. Army core enterprise services must be an easy-to-use, integrated suite of globally available, adaptable solutions that seamlessly supports the Army while working with unified action partners. To ensure that the Soldier is able to operate autonomously in austere environments, core enterprise services must take into account the unique requirements created by operations at the tactical edge. LOE 4 will provide these services to the Army in an adaptable way that maximizes efficiency, effectiveness and security, and ensures that information is available at the point of need to support critical decisions.

As network infrastructure and security are improved, the Army will implement Unified Capabilities, which comprise real-time communications via voice, video and data. This will be accomplished in coordination with DISA through the implementation of Voice over IP (VoIP) and sun-setting legacy analog telephone switches. VoIP will be integrated into a powerful suite of cloud-based collaboration tools for the warfighter and business user, including a single email address and phone number for the duration of the user's career. In the mid-term, core enterprise services will be expanded to include a portal to retrieve information end to end, from the enterprise to the tactical edge. These services will be made globally available and integrated to ensure that information is available at the point of need.

Modernized enterprise services will provide the Soldier and business user the ability to work in diverse environments without needing to learn how to use new services after each relocation to a new geographic location or organization. As a result, users will be more agile as mission needs evolve. Additionally, common collaboration services will help enable live, virtual and constructive training, split-base operations and global collaboration among regionally aligned forces.

LOE 5:
STRENGTHEN NETWORK OPERATIONS

Goal: Optimize end-to-end network operations by leading the development of data and resource strategies and policies, and an integrated architecture to establish common processes and standards, simplify and standardize capabilities, in support of and integrated with DoD Information Network Operations.

Desired End State: A resilient, protected, multi-tiered and rapidly configurable network that enables an information advantage for Army and Joint missions in cyberspace, supports Soldier requirements, and is responsive to the commander throughout all phases of operations and in all environments.

Objective 5.1: Improve and simplify network operation capabilities by converging to a single IT enterprise service management capability, reducing the complexity of designing, assembling, transporting and establishing mission-scaled networks and minimizing the burden on Soldiers.

Objective 5.2: Define analytical capability requisites to enhance spectrum monitoring, assignment and de-confliction.

Objective 5.3: Enable full situational awareness of networks by facilitating central oversight of critical network assets, health and mission readiness; and rapid integrated management and execution decisions regarding network resources and functions.

Objective 5.4: Enhance and extend incident response, audit, cybersecurity management and situational awareness services to the operating force.

Objective 5.5: Set strategic guidance by developing a single authoritative network operations concept of operations and information exchange specification framework.

The purpose of network operations is to assure system and network availability, information protection and information delivery to defend and maintain freedom of action within cyberspace for US/DoD/Army leaders. Army network operations is a subset of DoDIN operations and supports commanders at all levels by supplying situational awareness of the network, enabling mission command and providing the capability to monitor, detect, analyze, and respond to events and share information across the network.

The Army conducts network operations continuously in every theater through Regional Cyber Centers (RCCs), which are tasked to manage and defend mission-critical systems and ensure the continuity of network resources and functions in the face of disruption. RCCs and subordinate network operations entities must have standardized tools, tactics, techniques and procedures to be mutually supporting and achieve a common operating picture of the network at all levels. Additionally, due to the finite amount of available spectrum, the Army must leverage analytical capabilities and technology tools to enhance spectrum monitoring and optimize spectrum usage across the total force for operations and training. As the JIE concept matures, these capabilities will be largely delivered via a joint regional/functional Enterprise Operations Center (EOC) that incorporates RCC and a supporting Core Data Center (CDC). LOE 5 will work with stakeholders to produce and implement a single authoritative network operations concept of operations and information exchange specification framework, and to extend enterprise services to the operating force.

Implementation Way Ahead

Lines of effort are the mechanism by which the CIO/G-6 will work with stakeholders and mission partners to identify and execute key initiatives that support network end states in accordance with the Army Network Campaign Plan. The five lines of effort align with three Enterprise Information Environment Mission Area (EIEMA) domains which tie the Army's network investment priorities to Joint Capability Areas. Domains and initiatives are explained in detail, along with associated timelines and dependencies, in the Near- and Mid-Term Implementation Guidance.

Successful completion of key initiatives will enable the Army to divest and/or sunset legacy capabilities, and to set the conditions necessary to balance security with budget realities, operational effectiveness and efficiency.

Figure 5 depicts major initiatives grouped by LOE on an implementation timeline, which includes two critical periods: the near-term (the current year of execution and the President's Budget) and the mid-term (Program Objective Memorandum years).

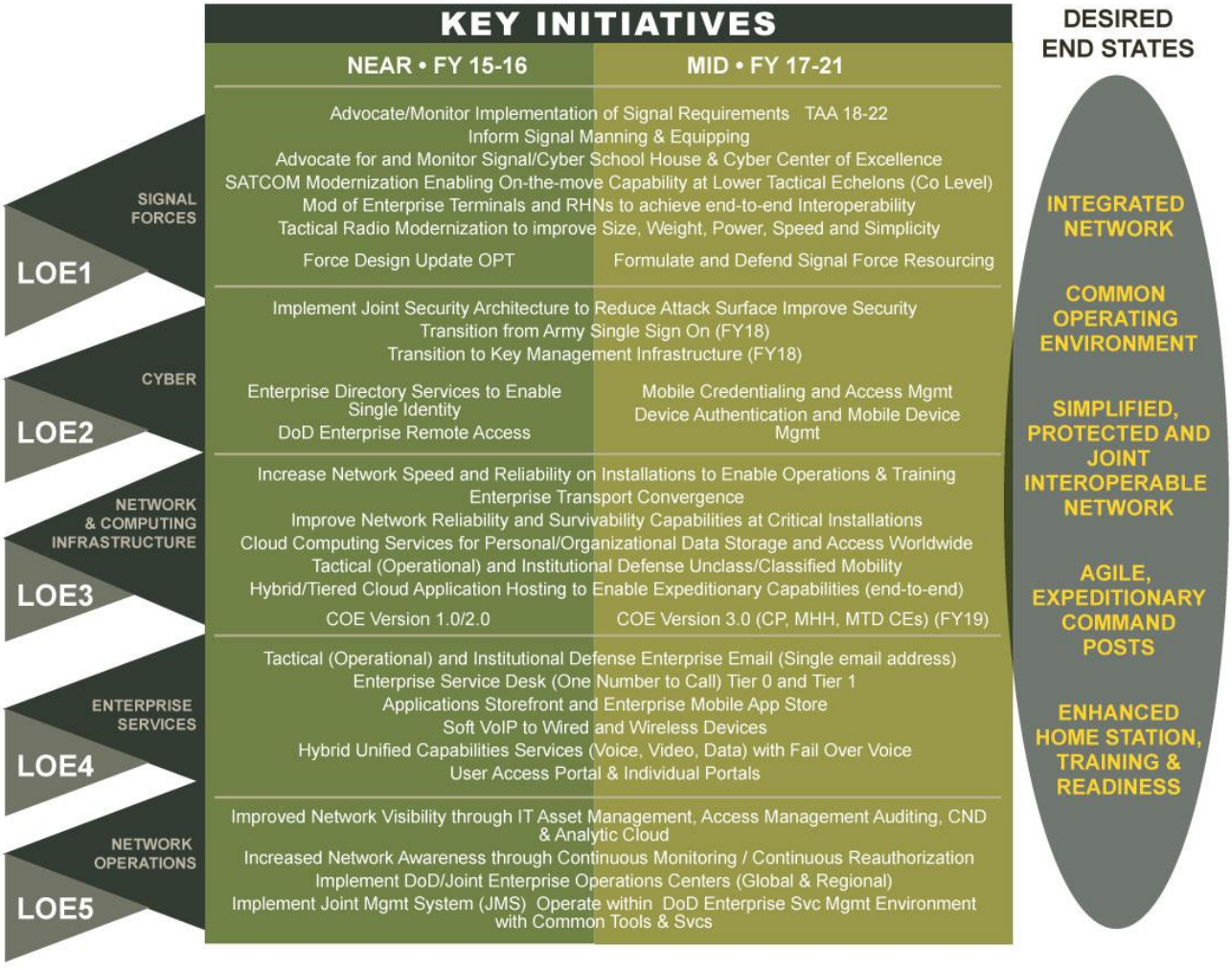


Figure 5: Network Initiatives Roadmap across the Near-Term and Mid-Term

Summary

The Army Network Campaign Plan supports The Army Plan by establishing priorities and focused efforts as Army IT stakeholders execute their roles and responsibilities. This plan:

- Defines our vision, mission and end states for the Army's Network 2020 and Beyond.
- Clarifies the strategic environment facing the Army in information technology.
- Outlines the CIO/G-6 LOEs and desired end-state objectives.
- Provides an Army Network Initiatives Roadmap to 2020 and Beyond.

The CIO/G-6 must work collaboratively with key stakeholders to ensure delivery of value-added information capabilities that enable mission command and ensure that our Soldiers maintain a technological advantage. We are enabling success for today and tomorrow by working together with our partners towards common end states for a modernized network that will better position the Army to support a regionally aligned, globally responsive force in a complex world.

This page intentionally left blank.

Acronyms

AEN	Army Enterprise Network
ANCP	Army Network Campaign Plan
AONS	Architecture, Operations, Networks and Space Directorate
CCoE	Cyber Center of Excellence
CO	Cyberspace Operations
COE	Common Operating Environment
CIO/G-6	Chief Information Officer/G-6
DCO	Defensive Cyberspace Operations
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership, Facilities, and Policy
DRU	Direct Reporting Unit
EIEMA	Enterprise Information Environment Mission Area
EUD	End-User Device
IdAM	Identity and Access Management
ISCM	Information Security Continuous Monitoring
IT	Information Technology
JCA	Joint Capability Area
JMS	Joint Management System
JRSS	Joint Regional Security Stack
LOE	Line of Effort
MPLS	Multi-Protocol Label Switching
OCO	Offensive Cyber Operations
P&R	Policy and Resources Directorate
RCC	Regional Cyber Center
UC	Unified Capabilities
VoIP	Voiceover IP